Remarks and Arguments

Reconsideration is respectfully requested.

Claims 1-12 are pending in the present application before this amendment. By the present amendment, claims 1 and 6 have been amended. No new matter has been added.

In the final office action (page 4), claims 1-12 stand rejected under 35 U.S.C. §102(a) as being anticipated by "NETASQ IPS-Firewalls. ASQ: Real-Time Intrusion Prevention" (ASQ V.2).

The applicants respectfully disagree and submit that claims 1 and 6 as presently amended are in condition for allowance over ASQ V.2.

Claim 1 has been amended and now recites in part:

> --wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and **dynamically** attaches said secondary connections to the authorization for connection of said main connection--.

Claim 6 has also been amended and now recites in part:

> –iv. means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol, **and wherein said unit for verifying the conformity of the communication flowing in a given connection, called main connection, to the said protocol, comprising means of detection of the data necessary for opening secondary connections induced by said main connection, and of attachment of said secondary connections to the authorization for connection of said main connection**–.

The applicants respectfully reiterate the applicants' earlier submission that the claimed method of claim 1 and the claimed device of claim 6 allow prevention of intrusion by detecting them **before penetration of the network.**

The examiner cites ASQ V.2, against the preambles of claims 1 and 6. However, ASQ V.2 discloses "NETASQ IPS-Firewalls are able to pro-actively break illegitimate sessions before the **last** packets are transmitted, therefore preventing attacks" (emphasis added). The phrase "**last** packets" does not disclose –the prevention of

intrusions-- because some of the packets may be potentially transmitted before a session is blocked.

Further, the screen shots and the text of ASQ V.2, page 8, both fail to illustrate that the intrusions are prevented by detection before penetration of the network. In fact, as the heading "Real-time **Monitoring** and Historical Logging" of ASQ V.2, page 8, indicates, the passages are disclose the act of monitoring and **not** --preventing intrusion--. As ASQ V.2, page 8, middle paragraph, discloses an overview of "current attacks being blocked," but does **not** disclose that the blocking of the attack is performed **before** intrusion in all instances.

The applicants also reiterate the applicants' earlier submission that secondary connections induced by a main connection are dynamically attached to the authorization of the main connection. The applicants further clarify this aspect of the presently claimed invention by the amendments to claim 1 and 6 as recited above. Support for the amendment to claim 1 can be found in paragraph [0051] of the application as published. The amendment to claim 6 refers to a device with claimed features in line with the features of method claim 1.

ASQ V.2 does **not** disclose that the secondary connections induced by each main connection are opened based on data coming from the performed conformity check, and are --dynamically attache[d] . . . to the authorization for connection of said main connection--.

In fact the disclosure of stateful inspection, ASQ V.2, page 4, is **not** comparable to detecting, by conformity checking, the data necessary for opening secondary connections induced by a main connection, and is **not** comparable to --attach[ing these] secondary connections to the authorization. . . of said main connection--.

Further, the disclosure of stateful inspection technology is simply a mention of a known technology that was also presented as prior art in the present application.

The applicants finally address that ASQ V.2 refers to an initial version of the ASQ

product, which does not implement all the claimed features of the product.

The new ASQ product, which implements the product's claimed features, now has the combined capacities to: recognize the accessing protocol, independently of the communication port used by this protocol; verify the conformity of each communication, flowing in a given connection, to the recognized protocol, layer by layer; deliver or withhold an authorization; and attach secondary connections induced by one main connection to the authorization of the main connection (where all these combined capacities can be done before the first passage of all the packets).

A device such as the one described directly above, allows "on the fly" real time analysis of the data, without any communication cut, whereas a proxy cuts the traffic and requires a connection management which is performed at the expense of the performance of the device. Proxies of this sort sometime create performance losses of 90%.

The combined features of the presently claimed invention achieve a high security level while maintaining performance.

Accordingly, the applicants respectfully submit that ASQ V.2 does not teach or disclose each element of the present invention of claims 1 and 6. Because the presently claimed invention is not anticipated by ASQ V.2, an indication of allowable subject matter with respect to claims 1 and 6 is respectfully requested.

Regarding claims 2-5, the applicants respectfully submit that claims 2-5 are allowable at least since they depend from claim 1, which is now considered to be in condition for allowance for the reasons above.

Regarding claims 7-12, the applicants respectfully submit that claims 7-12 are allowable at least since they depend from claim 6, which is now considered to be in condition for allowance for the reasons above.

In the office action (page 7), claims 1-12 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,174,566 (Yadav).

In continuation of the arguments presented above with respect to claims 1 and 6, the applicants disagree and assert that Yadav similarly does not anticipate the presently claimed invention.

In regards to the presented arguments discussing the prevention of intrusion by detection **before** penetration of the network. Yadav, Fig. 2A and 2B, as cited by the examiner, do **not** disclose the prevention of intrusion by detection **before** penetration of the network. As known in the art related to IDS systems, the system described in Yadav **monitors** traffic and allows at least part of the traffic flow before blocking occurs. As stated in Yadav, column 5, lines 3-4 and lines 37-45, the aim of the Yadav system is mainly to **monitor** the traffic.

Even if the Yadav system is capable of blocking traffic, Yadav does not disclose the ability to block traffic without the potential of allowing part of the traffic to enter the network. Specifically, Yadav, column 6, lines 33-37, discloses that the packets are checked to see if they "match a channel opened by the application rule enforcer," indicating that the packets are checked to see if they match an **already opened** channel.

In continuation of the arguments presented above regarding the present amendments to claims 1 and 6, Yadav, Fig. 3, as cited by the examiner, does not disclose that the secondary connections induced by a main connection are attached to the authorization of said main connection, after the data necessary to open said secondary connections are detected.

In fact, Yadav, Fig. 3 and corresponding specification as cited by the examiner, discloses an application rule enforcer (ARE) that aims at identifying an invoked application. Therefore, the ARE analyzes the full path of the lading application executable and the machine instructions embodying the application. The identification may be crosschecked with file properties information (name, size, version). Once the invoked application is identified, an application specific network policy is loaded and the ARE enters an idle state. The network I/O request made by the application is compared with the application specific network policy. The applicants respectfully submit that this

does **not** disclose the dynamic management of secondary connections induced by a main connection.

Accordingly, the applicants respectfully submit that Yadav does not teach or disclose each element of the present invention of claims 1 and 6. As the presently claimed invention is not anticipated by Yadav, an indication of allowable subject matter with respect to claims 1 and 6 is respectfully requested.

Regarding claims 2-5, the applicants respectfully submit that claims 2-5 are allowable at least since they depend from claim 1, which is now considered to be in condition for allowance for the reasons above.

Regarding claims 7-12, the applicants respectfully submit that claims 7-12 are allowable at least since they depend from claim 6, which is now considered to be in condition for allowance for the reasons above.

For the reasons set forth above, the applicants respectfully submit that claims 1-12 pending in this application are in condition for allowance over the cited references. Accordingly, the applicants respectfully request reconsideration and withdrawal of the outstanding rejections and earnestly solicit an indication of allowable subject matter. This amendment is considered to be responsive to all points raised in the office action. Should the examiner have any remaining questions or concerns, the examiner is encouraged to contact the undersigned attorney by telephone to expeditiously resolve such concerns.

Respectfully submitted,

Dated: 23 June 2009

W. William Park, Reg. No. 55,523
Ladas & Parry
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300